IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 09-13
www.iosrjournals.org

Verbal Authentication for Personal Digital Assistants

Aaroh Gala[1], Devang Mistry[2], Somdev Mehta[3], Manish Potey[4]
[1]*(Department of Computer Engineering, K. J. Somaiya College of Engineering, India)*
[2]*(Department of Computer Engineering, K. J. Somaiya College of Engineering, India)*
[3]*(Department of Computer Engineering, K. J. Somaiya College of Engineering, India)*
[4]*(Department of Computer Engineering, K. J. Somaiya College of Engineering, India)*

Abstract: *Personal Digital Assistant (PDA) i.e. a handheld device interacting with human beings verbally and performing tasks that are usually performed by an assistant, has been a growing and continuously evolving technology in recent years. Technology is rapidly automating all the manual work. In such scenario, the concept of PDA where everyone can carry their very own assistant in their pockets and can use it anytime and anywhere without even having to reach their pockets (i.e. completely hands-free usage) proves out to be a great success for technological world. There is no doubt about the fact that PDAs are the future of technology as all the major tech giants like Google, Microsoft, Apple etc. are keen on building and developing their own PDA. Thus, this advancement, demands for a reliable verbal authentication measure where a user can authenticate himself just by talking to the system. Moreover, this conversation should be such that, no intruder or attacker must be allowed to bypass the system even if he listens to the conversation that took place between the user and the PDA. This paper focuses on the security mechanisms that can be used to develop a base for verbal authentication and how it can be used as a powerful tool for validating login for device.*

Keywords: *PDA - Personal Digital Assistant, STT - Speech to Text, TTS- Text to Speech, API - Application Program Interface.*

I. Introduction

A Personal Digital Assistant (PDA), also known as a handheld PC, or Personal Data Assistant, is a mobile device that functions as a personal information manager. Most PDAs can synchronize their data with applications on a user's mobile. Hence it can synchronize the user’s data like events, birthday, reminders, alarms etc. And use this data to notify the user about it. It is not only restricted to this, since the main aim of PDA is to use it hands free, the user not only set reminders and alarms without using hands, but also perform multitask simultaneously like cooking and reading the notifications, or driving and getting the directions verbally without looking at the device etc.

The advancements in the technology of Personal Digital Assistants requires complete shift from textual data feeding to verbal data feeding. In other words, the manual work of feeding the data by typing must be transformed into simple voice commands where data is feed into the system verbally. This implies that, all the security and authentication measures must also be done over voice i.e. verbally. However, verbal authentication means disclosure of user information as verbally spoken things can be heard by surrounding people [2]. Furthermore, Verbal password highly relies on voice recognition, which isn’t highly secure and can be easily bypassed by various mechanisms [1]. Thus, the authentication mechanism must not be the same for every login unlike standard textual password authentication process where the same textual password is required for every login. Hence, the aim is to develop a procedure which enables credentials exchange and verification over voice.

II. Literature Survey

Personal Digital Assistants is one of the most promising upcoming technology. The research in this field is going with full acceleration. Every Major company is working on their own personal digital assistants. The tech giants are competing with each other to build the best PDA. Few examples of PDAs of well-known companies are as follows:

- GOOGLE NOW by Google
- SIRI by iPhone
- CORTANA by Microsoft
- ECHO and ALEXA by Amazon
- MOTO VOICE by Motorola

Not only this, but many people are working on their own customize PDA using Raspberry Pi, Banana Pi etc.
However, with the advent of new technology comes the risk of attack. Thus security is essential in every phase of a software. The existing systems, basically uses two types of security.

1. Verbal Password.
2. Voice Recognition.

1. Verbal Password:

In this mechanism the user need to speak out the password, or spell out the characters or numbers of the word which is the password or pin of the system. And the system will check whether the user said the correct password or not and authenticate the user.

2. Voice Recognition:

In this system the user need to speak a phrase or speak something, and the device will recognize the pattern and the frequency of the voice, and will compare it with the voice pattern and frequency of the voice recorded while registrations and on the basis of that the user is authenticated[3]. In this system the user is given a leverage of slight variation in the pattern and frequency.

III. Limitations Of Existing System

The existing system uses two main methods for security and both the mechanisms have certain limitations. The limitations are as follows:

1. Verbal Password:

In this mechanism the user needs to speak out the password or pin or the characters of the string. It is one of the less secure system, as this works best in the scenario when the user is alone, or in private place[5]. But if the user is in public or in crowded environment, then people around the user can hear the password. This could lead to easy bypassing the system once a person hears the password[1]. Also, this password could be guessed by the closed ones, as people generally tend to keep passwords which are easy to remember like birthday, or name, or anniversary, or partner's name etc. Hence, it is easy to bypass this system for a person who is close to the user.

2. Voice Recognition:

In this mechanism the user’s speech pattern and the voice frequency comes into picture for authentication. But according to the research by Jean-François Bonastre, Frédéric Bimbot, Louis-Jean Boë, Joseph P. Campbell, Douglas A. Reynolds, Ivan Magrin-Chagnolleau who published a paper called “Person Authentication by Voice: A Need for Caution” in an International Journal, voice recognition is vulnerable and it’s not a reliable technology[4].

Certain points covered in the paper are, that the device won’t be able to recognize whether the voice is spoken by a person the voice is disguised by someone else. Other point was covered that since the device cannot recognize the person, hence a recording of the person’s voice can also bypass the system [4]. Finally, a person with similar voice pattern can easily bypass the system which uses voice recognition.

IV. Proposed System

After studying the existing system’s security mechanism, we can say that the security of the current system is not reliable and secure. And since this technology is one of the most promising upcoming technology which interacts with the user’s data. Hence, Security should be strong and reliable. The main aim is to enhance the security of PDAs so that they can be use anywhere without the risk of letting nefarious people know the passwords while using it in public place, and keeping the system more secure as well as the user’s data.

From the limitations of the existing system, we know that there is a need of adding another layer of authentication so as to keep system more secure.

This is resolved using two mechanisms:

- **Challenge-Response:**

In this technique the user needs to define a set of questions along with its respective answers. Generally, this set of questions will be 15-20 basic questions. This will be done while registration. During login, the user will be asked a set of random questions (generally 3 questions), which will be randomly selected and those questions will be asked to the user. If the user answers those questions correctly, then he can be authenticated. Since the user is asked random questions, whose answers are known only to the user, gives an addition of security as it may take time by other to guess the answer.

Also to bypass of the security by recording the voice password can be avoided as the set of questions are randomly selected, and a person won’t be able to record each and every answers of all the questions. Hence the bypass by recorded voice is avoided here.

- **Self Learning Mechanism:**

From the above mechanism, one can argue that a person very close to the user may know answer to all the registered questions. Therefore, this mechanism is added to overcome the same. In this mechanism, the system will learn from the user's recent activities from various accounts that he uses. For e.g. New friend added on Facebook, or Google Circle recently etc.

Hence, the questions are created dynamically by the system based upon user's activity whose answers are supposed to be known by users only. The close one won't be updated with day to day life of the user. Thus the proposed system not only provide us with a complete hands-free interaction with PDAs i.e. Communication with the PDA can be done even if the device is at a distance from the user. Also the reliability of the system on voice recognition is reduced along with making the system more secured. Since the security of the system is more secured and reliable, hence we can use this as a single authentication system to authenticate multiple devices connected to the same network.

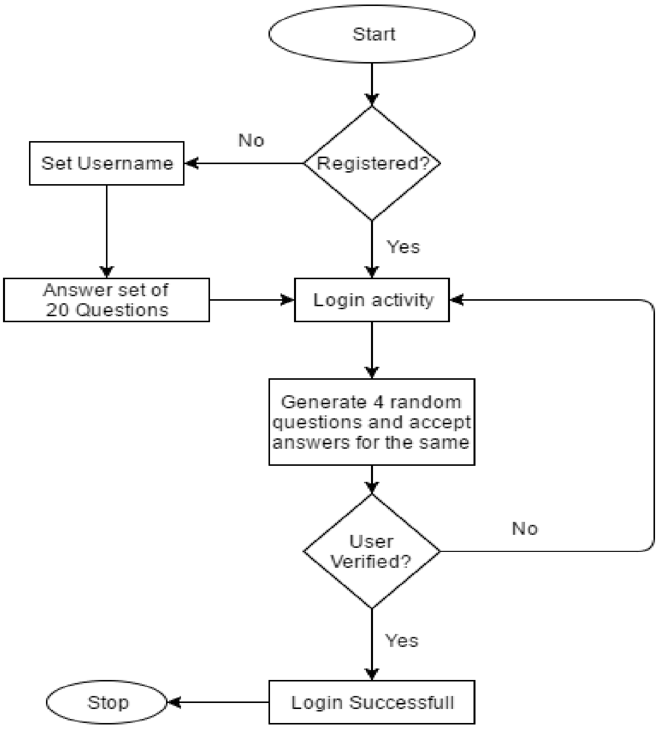


Fig 4.1- Flowchart of the proposed system.

V. Implementation

An Android Application is made of this. When the user opens the he/she would see the first screen shown in Fig 5.1

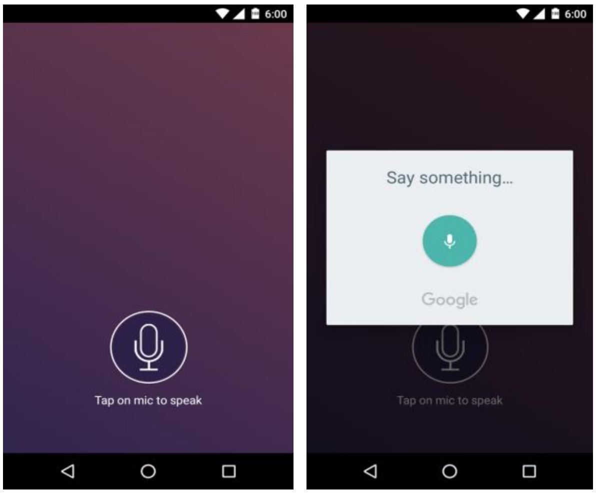
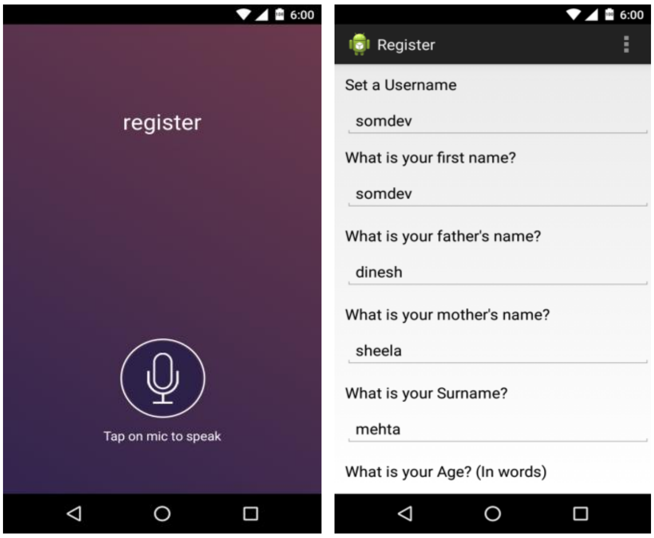


Fig 5.1 – Main Screen

The user can ask basic questions and task like setting an alarm, reminder, get the weather information etc. To register, the user needs to create an account. This can be done by saying “Register”. When the user says register, the Main Screen shown in Fig 5.1 will redirect the user to Register Screen as shown in Fig 5.2.



Set a Username

somdev

What is your first name?

somdev

What is your father's name?

dinesh

What is your mother's name?

sheela

What is your Surname?

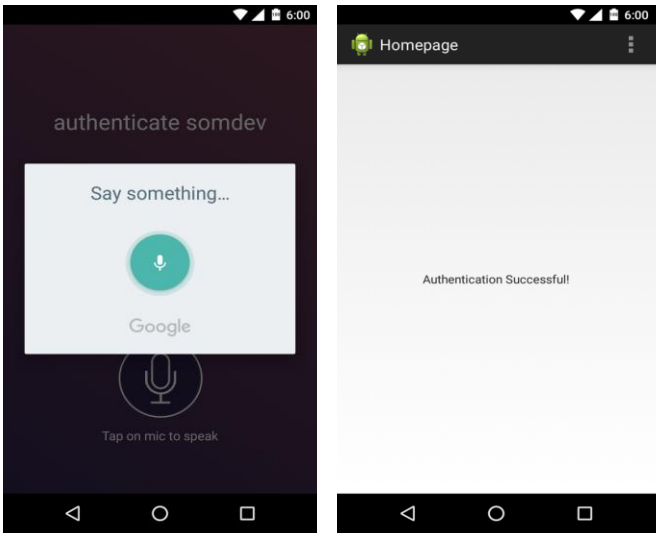
mehta

What is your Age? (In words)

Fig 5.2 – Register Screen

The user needs to set a username and answer set of basic questions, which will be used to authenticate the user. The user needs to type the answers of the basic questions. Once the user has set the username and answered the basic questions, the user’s account will be made. The details of the account and answers are stored in tables using SQL. The database is hashed using MD5 Hashing for security.

Once the user account is created, he can authenticate himself by saying “Authenticate” or “Authenticate username” on the Main Screen.



Authentication Successful!

Fig 5.3- Authentication Screen

Once the user says authenticate, the system will ask the user name. Then the system checks the username in the table, if the username is not available then the system responds “Username not found”. If the username entered is correct, then the system will select 4 random questions from the database and ask the user. The user is given the privilege to answer a question for maximum 3 times, by considering that the system interprets wrong due to noise or user misspelled the answer. If the user answers wrong for more than three times, then the user needs to authenticate again from the start. Once the user answers all 4 questions correctly, then the user is authenticated.

VI. Conclusion

The need for the transformation from text based data feeding to voice based data feeding is the dawn of a new technology which will require security and authentication over voice. The proposed system very well determines all possible loopholes that could be generated with this transformation and alleviates the same using challenge response and self-learning mechanisms. Also, the fact that voice recognition is still in its infant stage, is very well adopted by the system as it aims to act like a second level of authentication ensuring that unauthorized breach never occur even when voice recognition fails.

References

[1] Sarabjeet Singh, Yamini M “Voice Based Login Authentication For Linux” in 2013 International Conference on Recent Trends in Information Technology (ICRTIT).

[2] R.C. Johnsona,b, Walter J. Scheirera,c and Terrance E. Boulta,b “Secure voice based authentication for mobile devices: Vaulted Voice Verification” in 2012.

[3] Dong-Ju Kim, Kwang-Woo Chung, and Kwang-Seok Hong “Person Authentication using Face, Teeth and Voice Modalities for Mobile Device Security” IEEE transactions on Consumer Electronics, Vol 56, No.4 November 2010

[4] Jean-François Bonastre, Frédéric Bimbot, Louis-Jean Boë, Joseph P. Campbell, Douglas A. Reynolds, Ivan Magrin-Chagnolleau “Person Authentication by Voice: A Need for Caution” in EUROSPEECH 2003: GENEVA.

[5] Qi Li, Biing-Hwang Juang, Qiru Zhou and Chin-Hui Lee “Automatic Verbal Information Verification for User Authentication” in IEEE TRANSACTIONS ON SPEECH AND AUDIO PROCESSING, VOL. 8, NO. 5, SEPTEMBER 2000.